Follow us
On Twitter

April 2015 Issue

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

DTI *e*Security News — Data Breach Fatigue

Suffering from Breach Fatigue?

Another day, another report of a data breach in banking, retail or healthcare. It seems just a part of daily life. More than 76 million were affected by the JP Morgan breach, and 53 million credit/debit cards were compromised at Home Depot. Yet both of these institutions reported an uptick in earnings in the final quarter of 2014. It appears that these companies were not negatively affected in a financial way by the breaches, and IT security experts are perplexed as to why.

Data breaches were up over 25% in late 2014, compared to the same time period the previous year. At the end of 2014 there were more than 600 breaches reported, equal to about two per day. This constant pace and media reporting has contributed to something called **'data breach fatigue.'**

A Ponemon Institute report states that one-third of consumers completely ignored data breach notices, doing nothing, and more than 50% did not take a single step to protect themselves from future identity theft attempts. Why are we becoming so complacent about the risks to our personal information?

These results can be viewed in two ways: either victims lack the energy or resources to change their behavior or they just accept that breaches are now the norm. Since the financial losses are generally minimal, many don't see any reason to worry about new breaches that will occur and may be inclined to simply ignore future announcements.

HERE'S THE PROBLEM: if we as consumers don't care, why should companies worry about security?

Visit our Cyber Security website for previous issues of *e*Security Newsletters

What are the Consequences?

- The average time before a breach is discovered is almost seven months. The longest a breach went undiscovered is 2,982 days, or about *eight years!*
- 69% of breaches were discovered by an outside source, not the company or retailer themselves.

Current security measures are not enough, and the hackers are getting better at hiding malware and other cyber attack tools. Either way, the threats are real and increase daily.

If consumers are not vigilant and do not respond to breach notices and take precautions, what incentive is there for companies to continue their cyber security investments?

Who pays for data breaches? That's hard to decipher, too. Retailers place the burden on the credit card companies. Consumers generally suffer small financials burdens, and credit card companies are slow to change their cards to the more secure computer chip and PIN Cards.

What Can I Do?

- **Don't become apathetic.** Be a cyber savvy consumer.
- **Monitor your accounts and credit statements diligently.** Change your passwords regularly.
- **Respond to each and every breach notification you receive**. If you read about a breach and haven't received notice, do not hesitate to contact your financial institution.
- **Find out when your credit card issuer will offer computer chipped PIN cards.** They are already the norm in Europe, and U.S. retailers are required to install chip and PIN compatible card readers at stores by October 2015.

For more information on family cyber safety, please go to: http://dti.delaware.gov/information/cybersecurity.shtml.

Questions or comments?
Email us at eSecurity@state.de.us

SECURITY - *Now ...more than ever!*
Cyber Security - Disaster Recovery - Continuity of Government